Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Некоторые особенности архитектуры высокоскоростных средств шифрования для обеспечения криптографической защиты центров обработки данных

МАРЕЕВА ЕЛЕНА ВЛАДИМИРОВНА

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО НТР

СИСТЕМЫ ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

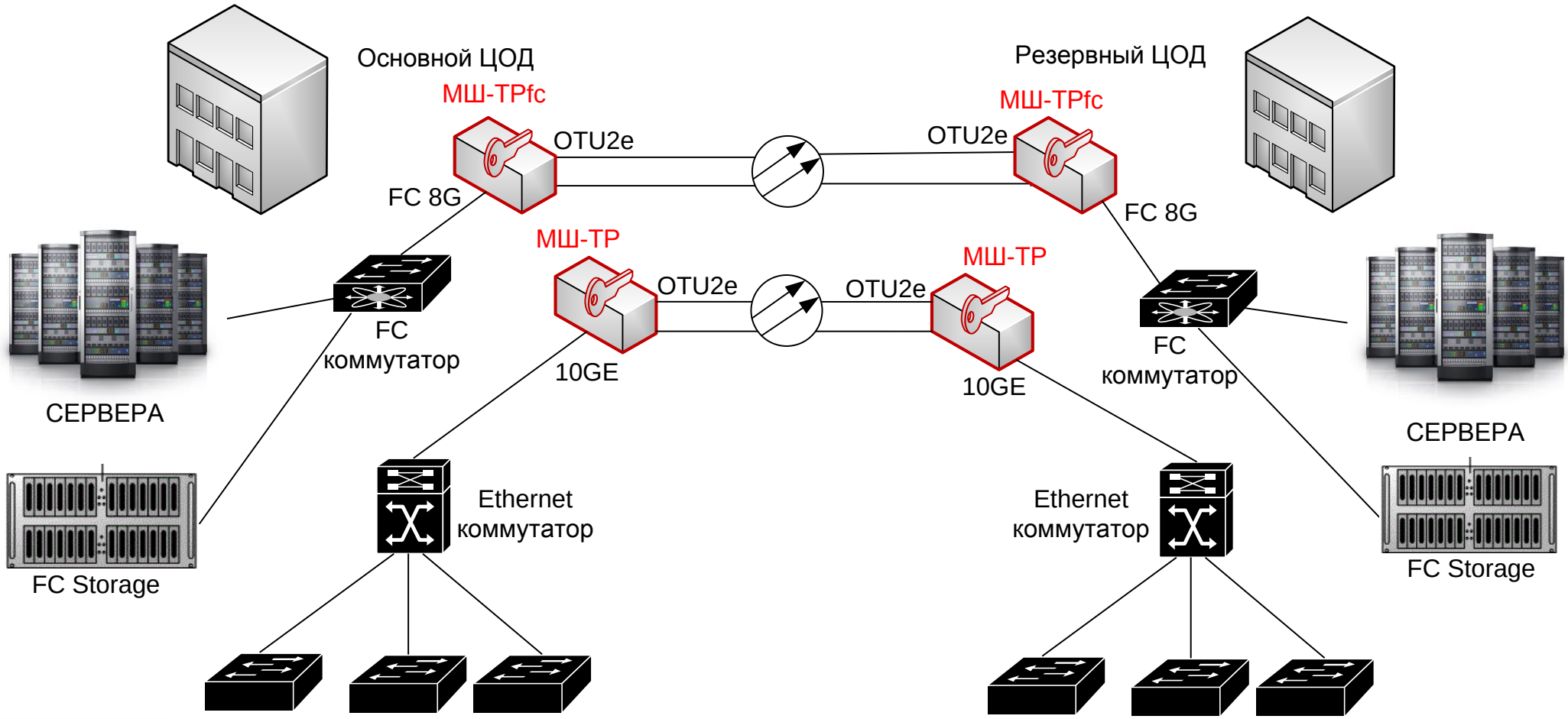
Цель и технологии

Криптографическая защита центров обработки данных – это защита информации, передаваемой между ЦОД по оптической транспортной сети (OTN) с технологией спектрального уплотнения (DWDM), в том числе при использовании распределённой архитектуры построения ЦОД - Storage Area Network (SAN)

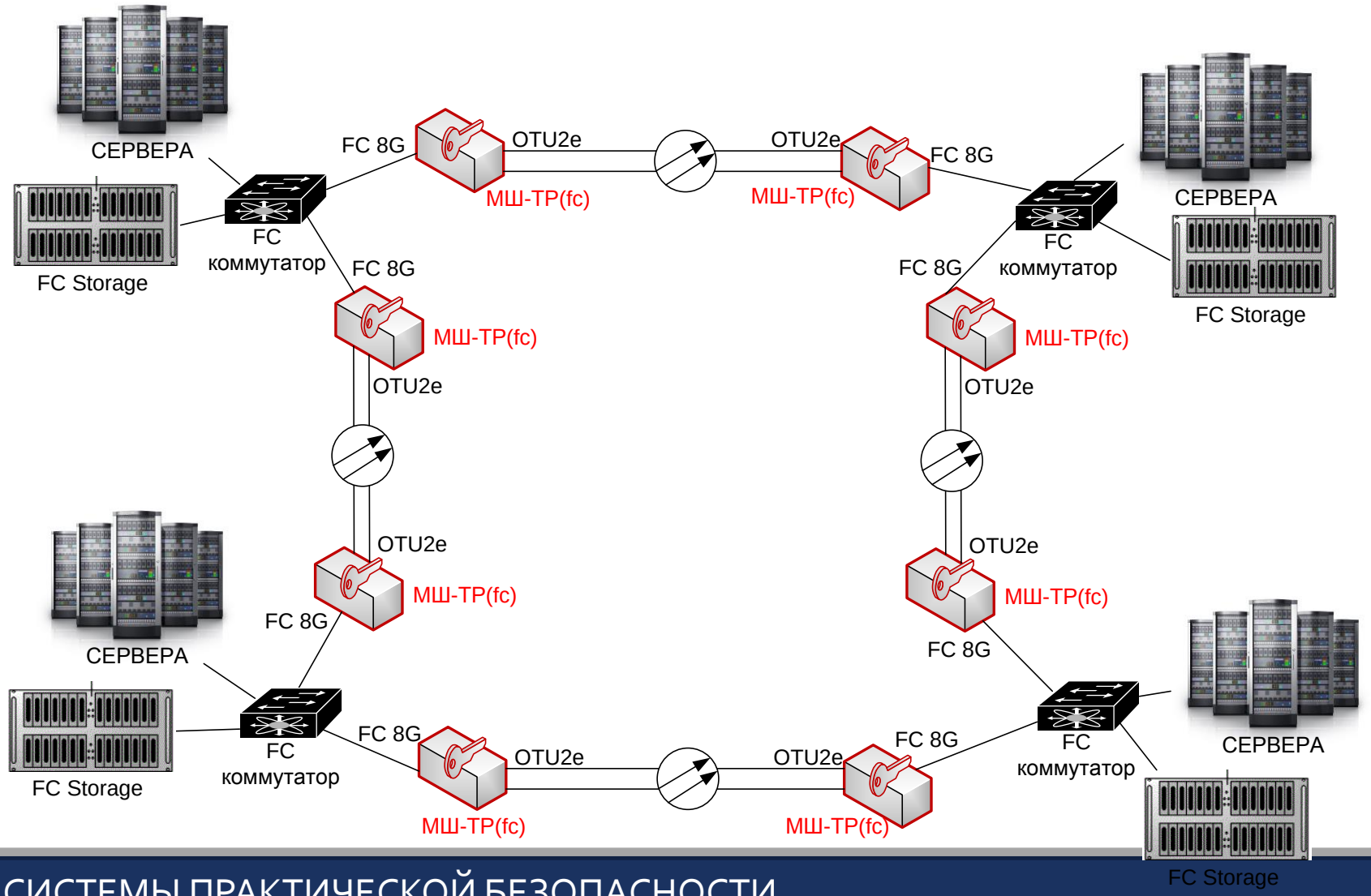
В настоящее время при построении сетевой инфраструктуры ЦОДов, в основном, одновременно используются технологии передачи данных Ethernet, Fibre Channel, OTN и DWDM

Криптографическая защита информации ЦОД – это обеспечение конфиденциальности передаваемых данных (шифрование) и защита от навязывания ложной информации (имитозащита)

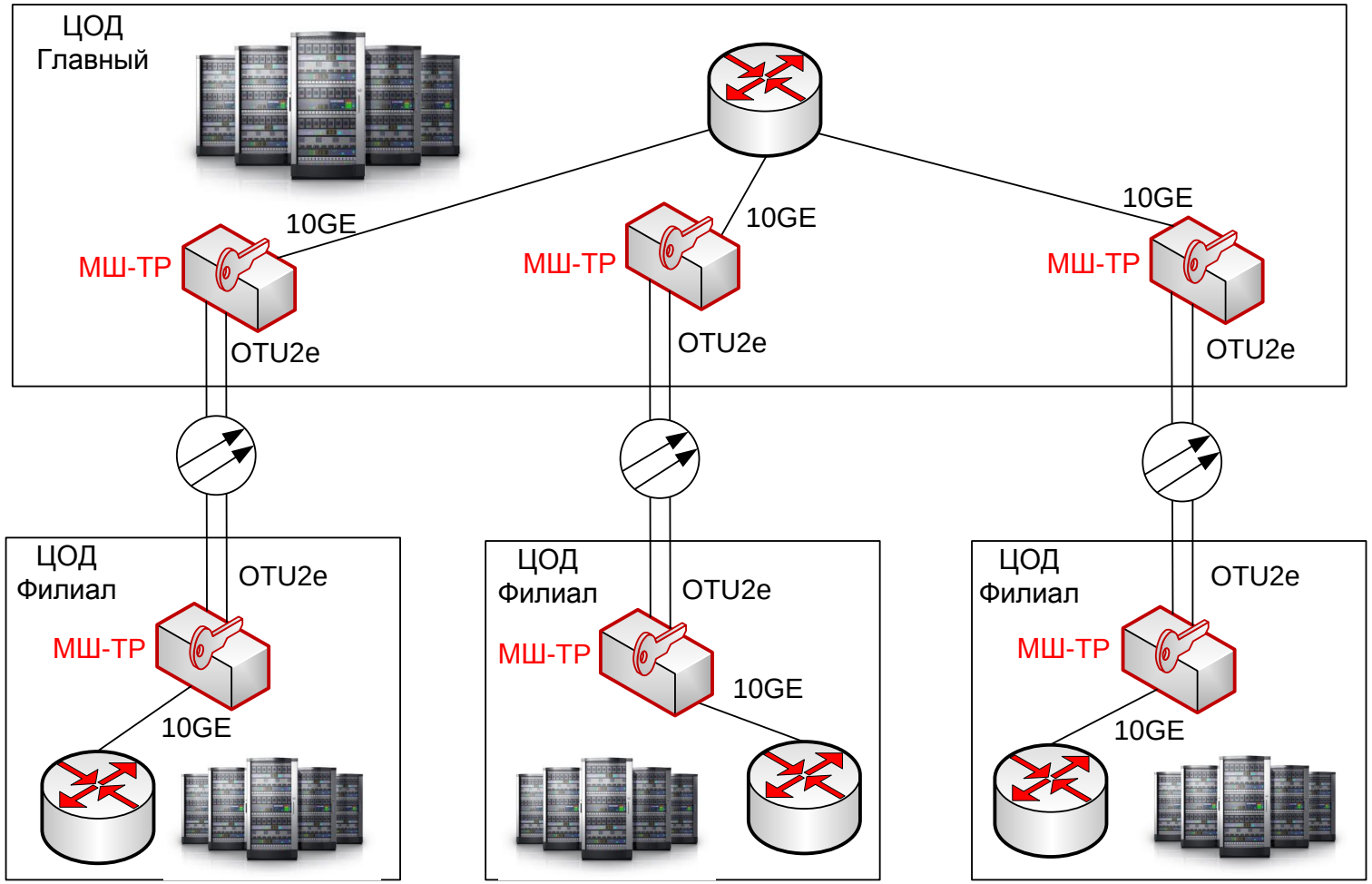
Взаимодействие ЦОД . Резервирование



Взаимодействие ЦОД. SAN сеть



Взаимодействие ЦОД. Сбор данных



Требования к СКЗИ для ЦОД

Базовые функциональные требования: шифрование и имитозащита

Дополнительно должны обеспечиваться:

- ✓ высокая пропускная способность: 10, 40, 100 Гбит/с
- ✓ отсутствие потерь пакетов защищаемой информации при различных длинах пакетов
- ✓ минимизация латенсии и отсутствие её зависимости от длины пакетов защищаемой информации
- ✓ обеспечение возможности агрегирования и передачи по транспортной сети любых необходимых типов клиентских сигналов (STM, Ethernet, Fibre Channel)
- ✓ оперативное пополнение (соответствующее классу СКЗИ и пропускной способности) расхода большого объёма ключей
- ✓ высокая надёжность с возможностью автоматического перехода на резервную линию связи

СКЗИ уровень L3. Криптомаршрутизаторы или IP-шифраторы

\+ Обеспечивают межоконечное сетевое решение по шифрованию трафика, не зависящее от физической сети и установленного в ней оборудования

- Отсутствует поддержка не IP транспортных потоков, в том числе протокола средств хранения данных ЦОД Fibre Channel
- Требуют больших вычислительных ресурсов для обработки IP трафика (фильтрация, маршрутизация, фрагментация-дефрагментация)
- Требуются дополнительные накладные расходы, связанные с необходимостью обеспечить независимое шифрование (расшифрование) и имитозащиту (аутентификацию) каждого пакета и заключающиеся в увеличении размера пакета, что в свою очередь, приводит к увеличению задержки сети и потери части полосы пропускания на волоконно-оптических линиях

СКЗИ уровень L2. MAC-шифраторы

Шифрует данные, содержащиеся в Ethernet кадрах на точка-точка Ethernet соединениях

+ По сравнению с шифраторами L3 уровня имеет улучшение эффективности сети и латенсии, так как по сравнению с L3 шифраторами имеет меньшие по размеру дополнительные затраты на фрейм.

- исключает встроенную поддержку для всех не-Ethernet типов клиентов
- имеет ограниченную архитектуру точка-точка (или hop-by-hop), которая определена уровнем MAC, таким образом потенциально добавляя сложность сетевого планирования

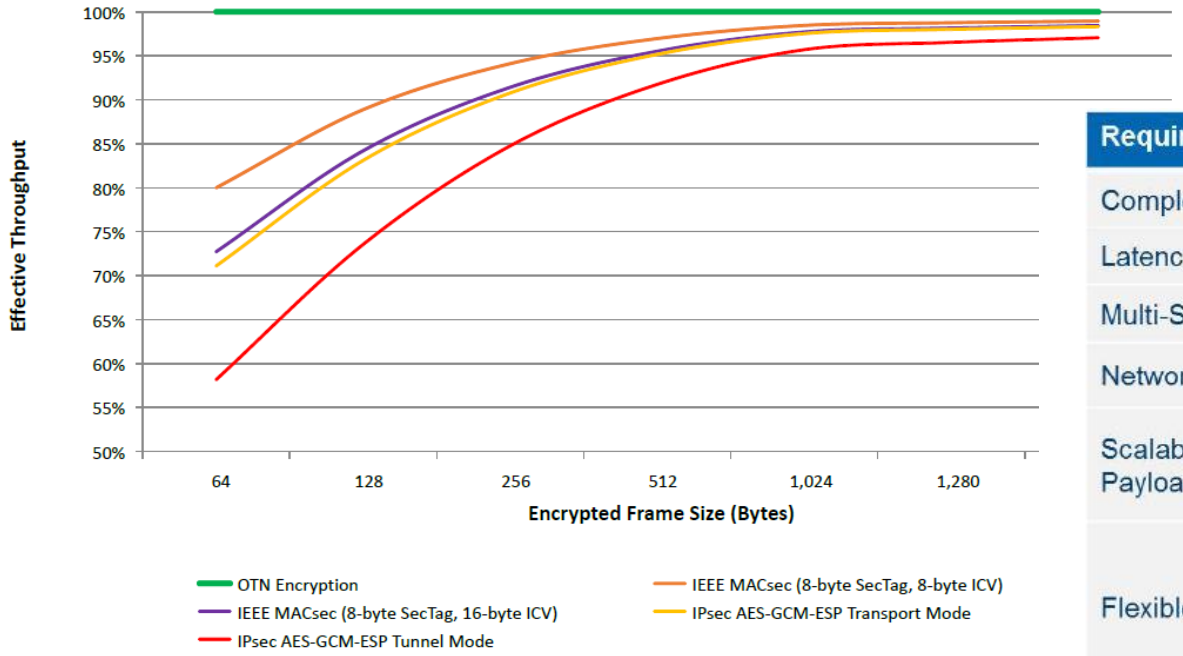
СКЗИ уровень L2/L1. Оптические шифраторы

Устройства данного класса не занимаются маршрутизацией, но могут агрегировать абонентскую информацию, получаемую даже из технологически разных сетей (пакетной сети и синхронной TDM сети) и передавать её до следующей точки оптической сети в виде шифрованных кадров формата OTU

- Низкая латенсия, не зависящая от характеристик клиентского трафика
- Отсутствие зависимости производительности от характеристик клиентского трафика и, как следствие, отсутствие потерь и максимальная производительность при криптоимитозащите
- Мультисервисность за счёт агрегирования абонентской информации и её конвергенции в протокол уровня L1
- Масштабируемость для шифрования полезных нагрузок
- Отсутствие сложности управления
- Являются оптимальным решением для сопряжения с системами квантового распределения ключей по критериям идентичности транспортной среды и требуемой производительности

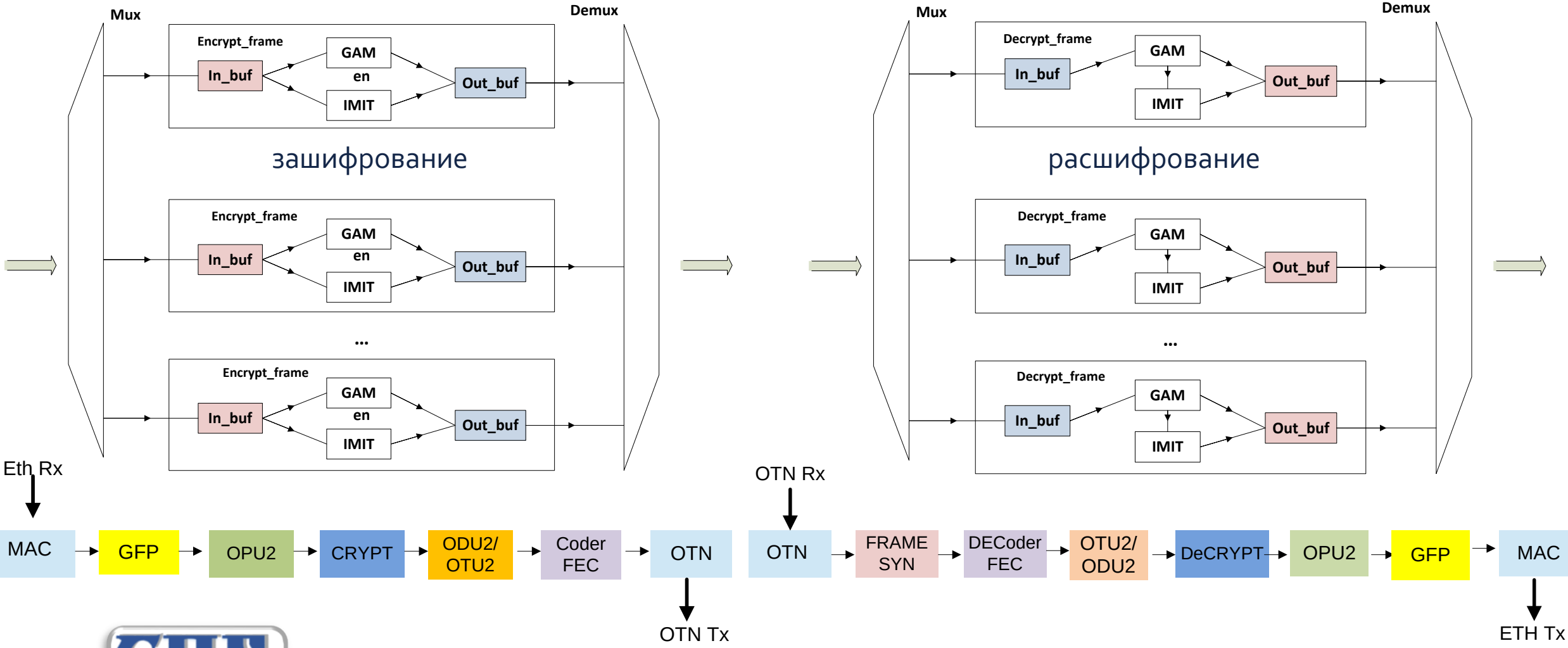
Сравнение классов СКЗИ (L3, L2, L1)

Figure 3 • Network Throughput vs. Encrypted Frame Size (Bytes)

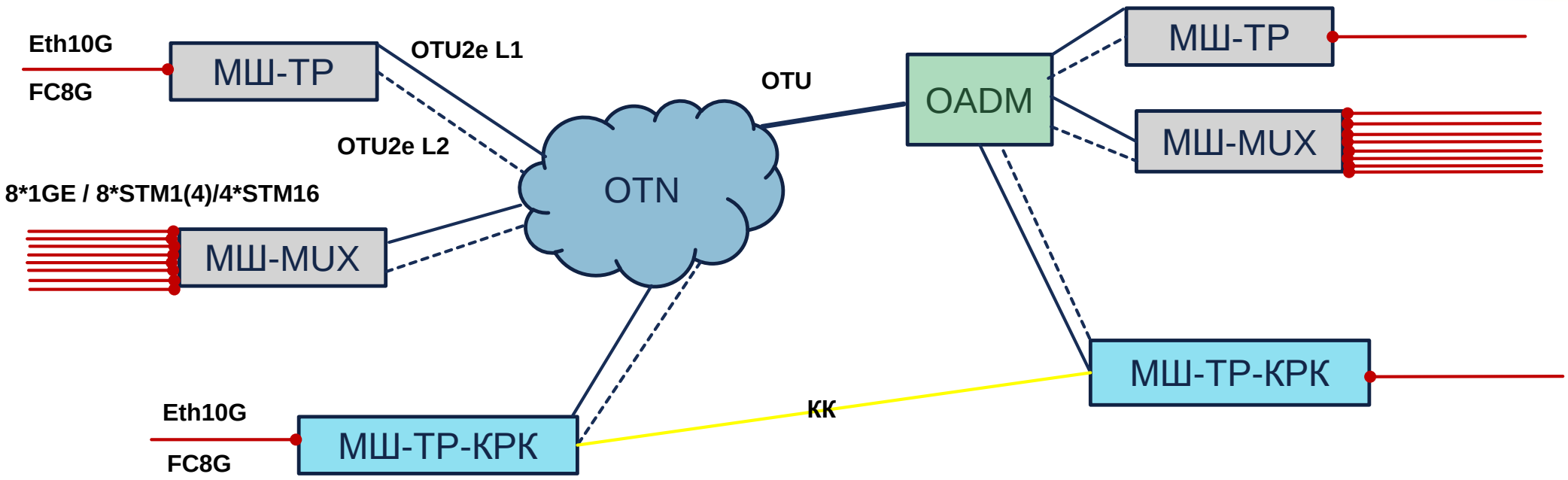


Requirement	IPsec (L3)	MACsec (L2)	OTN (L1) Encryption
Complexity & Cost	High	Low	Low
Latency	High	Low	Low
Multi-Service	No	No	Yes
Network Efficiency	Low	Medium	100%
Scalable Encrypted Payload Size	Restricted	Restricted *Standard MAC sizes*	Flexible *1.25G – 100G ODUflex*
Flexible Deployment	-	Low *Hop-to-Hop Only*	High *Wavelength Sub-Wavelength Point to Point WDM Layer 1 Switched*
End-to-End	IP Only	Layer 2 Only	Layer 1 OTN only

Архитектура СКЗИ уровень L2/L1



Характеристики линейки СКЗИ Квазар



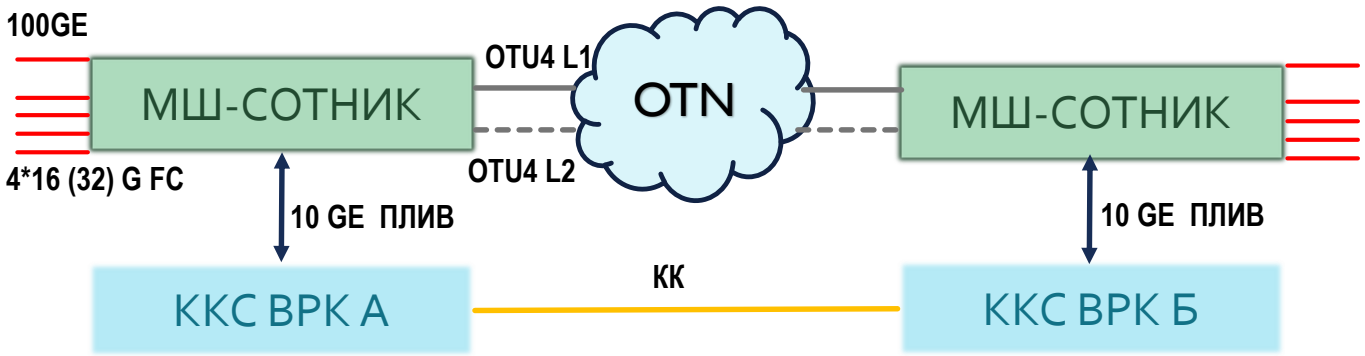
OADM –оптический мультиплексор DWDM

Характеристики линейки СКЗИ Квазар

Характеристика	МШ-ТР	МШ-MUX
Алгоритм шифрования	ГОСТ Р 34.12-2015 Магма, ГОСТ Р 34.13-2015 CTR	
Имитозащита	ГОСТ Р 34.13-2015	
Клиентские интерфейсы	10 Gbit Ethernet/ 8Gbit FC	8x1Gbit Ethernet / 8xSTM1(4)/4xSTM16
Линейные интерфейсы	2xOTU2e	2xOTU2e
Производительность	Без зависимости от размера клиентского фрейма	
	10Gbit Ethernet, 6,8Gbit FC*	8 Gbit Ethernet
Латенсия	0,05 мс	
Резервирование	Автоматическое переключение с L1 на L2 за время 50 мс	
FEC	ITU G.709	

* Максимальное значение для данного протокола и способа кодирования

Характеристики СКЗИ Сотник



Характеристика	СОТНИК
Алгоритм шифрования	ГОСТ Р 34.12-2015 Кузнечик, ГОСТ Р 34.13-2015 CTR
Имитозащита	ГОСТ Р 34.13-2015
Клиентские интерфейсы	100 Gbit Ethernet/ 4x16 Gbit FC/ 4x32 Gbit FC
Интерфейс ККС-ВРК	10 Gbit Ethernet
Линейные интерфейсы	2xOTU4
Производительность	100 Gbit Ethernet
	Без зависимости от размера клиентского фрейма
Латенсия	0,003 мс
FEC	ITU G.709
Резервирование	Есть

Контактная информация

Электронная почта:

mareeva@systempb.ru

Телефон:

+ 7 (812) 468-15-61, доб. 210

+ 7 (921) 301-92-70

Сайт: https://systempb.ru